International Journal of Pure and Applied Mathematics
Volume 77 No. 1 2012, 1-9
ISSN: 1311-8080 (printed version)
url: http://www.ijpam.eu

ijpam.eu

A GENERALIZATION OF THE ANOMALOUS ATTACK FOR THE ECDLP OVER $\mathbb{Q}_p$

Masaya Yasuda

Fujitsu Laboratories Ltd.
1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki
211-8588, JAPAN

Abstract: The elliptic curve discrete logarithm problem (ECDLP) over a field K is as follows: given an elliptic curve E over K, a point $S \in E(K)$, and a point $T \in E(K)$ with $T \in \langle S \rangle$, find the integer d such that $T = dS$. The hardness of the ECDLP over a finite field is essential for the security of all elliptic curve cryptographic schemes. Semaev, Smart, and Satoh and Araki independently proposed an efficient attack for the ECDLP over $\mathbb{F}_p$ in the anomalous case, which is called the *anomalous attack*. In this paper, we generalize the method of the anomalous attack and give an algorithm for solving the ECDLP over the p-adic field $\mathbb{Q}_p$.

AMS Subject Classification: 14G52, 11G07
Key Words: ECDLP, formal groups, the anomalous attack

1. Introduction

The elliptic curve discrete logarithm problem (ECDLP) over a field K is as follows: given an elliptic curve over K, a point $S \in E(K)$, and a point $T \in E(K)$ with $T \in \langle S \rangle$, find the integer d such that $T = dS$. The hardness of the ECDLP over a finite field is essential for the security of all elliptic curve cryptographic schemes, for example, elliptic curve-based signature, public-key encryption, and key establishment schemes [2]. In general case, no efficient algorithm is known

Received: May 16, 2011

for the ECDLP over a finite field. However, in the anomalous case, Semaev [6], Smart [8], and Satoh and Araki [5] independently proposed an efficient attack for the ECDLP over a finite field, which is called the *anomalous attack* [1]. In this paper, we generalize the method of the anomalous attack and give an algorithm for solving the ECDLP over the p-adic number field $\mathbb{Q}_p$.

Let p be a prime number and let E be an elliptic curve over $\mathbb{Q}_p$. Denote $\widetilde{E}$ the reduction of E modulo p and let $\pi : E(\mathbb{Q}_p) \to \widetilde{E}(\mathbb{F}_p)$ be the reduction map (see [7]). For simplicity, we assume that $\widetilde{E}$ is an elliptic curve over $\mathbb{F}_p$. Then we have an exact sequence of abelian groups (see [7])

$$0 \to \ker \pi \to E(\mathbb{Q}_p) \xrightarrow{\pi} \widetilde{E}(\mathbb{F}_p) \to 0.$$

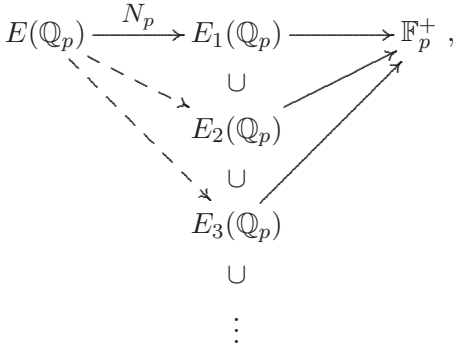
For $n \geq 1$, we define a subgroup $E_n(\mathbb{Q}_p)$ of $E(\mathbb{Q}_p)$ defined by

$$E_n(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) \mid v_p(x(P)) \leq -2n\} \cup \{O\},$$

where v_p is the normalized p-adic valuation and $x(P)$ is the x-coordinate of a point P. We note that $E_1(\mathbb{Q}_p)$ is equal to $\ker \pi$ and $E_1(\mathbb{Q}_p)$ is isomorphic to the group of $p\mathbb{Z}_p$-valued points of the formal group associated to E (see [7]). Although the group $E_1(\mathbb{Q}_p)$ is only considered in the anomalous attack, our idea is to use the filtration $\{E_n(\mathbb{Q}_p)\}_{n\geq 1}$ of $E_1(\mathbb{Q}_p)$ with

$$E_1(\mathbb{Q}_p) \underset{\mathbb{F}_p^+}{\supset} E_2(\mathbb{Q}_p) \underset{\mathbb{F}_p^+}{\supset} E_3(\mathbb{Q}_p) \underset{\mathbb{F}_p^+}{\supset} \cdots,$$

where $E_n(\mathbb{Q}_p)/E_{n+1}(\mathbb{Q}_p) \simeq \mathbb{F}_p^+$ for $n \geq 1$. In our method, we mainly consider the following diagram:



where N_p denotes the multiplication by $N_p = \sharp\widetilde{E}(\mathbb{F}_p)$ and the maps on the right hand side are induced by isomorphisms $E_n(\mathbb{Q}_p)/E_{n+1}(\mathbb{Q}_p) \simeq \mathbb{F}_p^+$. Using

the above diagram, we give an algorithm for solving the ECDLP over $\mathbb{Q}_p$. We note that the first horizontal map in the above diagram is a key tool for the anomalous attack. Therefore our method is a generalization of the anomalous attack with the filtration $\{E_n(\mathbb{Q}_p)\}_{n\geq 1}$ of $E_1(\mathbb{Q}_p)$.

The outline of this paper is as follows: In Section 2, we review on the method of the anomalous attack. In Section 3, we generalize it and give an algorithm for solving the ECDLP over $\mathbb{Q}_p$. In Section 4, we conclude our study.

2. Review on the Anomalous Attack

In this section, we briefly review on the method of anomalous attack due to [5].

Let p be a prime number and let $\widetilde{E}$ be an elliptic curve over $\mathbb{F}_p$. Fix an elliptic curve E which is a lifting of $\widetilde{E}$ to $\mathbb{Q}_p$ and let $\pi : E(\mathbb{Q}_p) \to \widetilde{E}(\mathbb{F}_p)$ be the reduction map (see [7, Chapter VII] for its definition). Then we have an exact sequence of abelian groups (see [7, Proposition 2.1 of Chapter VII])

$$0 \to E_1(\mathbb{Q}_p) \to E(\mathbb{Q}_p) \stackrel{\pi}{\to} \widetilde{E}(\mathbb{F}_p) \to 0,$$

where $E_1(\mathbb{Q}_p) = \ker \pi$. We note that the subgroup $E_1(\mathbb{Q}_p)$ of $E(\mathbb{Q}_p)$ is isomorphic to the group $\mathcal{E}(p\mathbb{Z}_p)$ of $p\mathbb{Z}_p$-valued points of the formal group $\mathcal{E}$ associated to E (see [7, §2 of Chapter VII] for details). Then we can consider a composition of the following maps

$$h : E(\mathbb{Q}_p) \stackrel{N_p}{\to} E_1(\mathbb{Q}_p) \simeq \mathcal{E}(p\mathbb{Z}_p) \stackrel{\log_E}{\to} p\mathbb{Z}_p \stackrel{\bmod p^2}{\to} \mathbb{F}_p^+,$$

where N_p denotes the multiplication by $N_p = \sharp\widetilde{E}(\mathbb{F}_p)$ and $\log_E$ denotes the formal logarithm of $\mathcal{E}$. We note that the map h is a group homomorphism.

For any lifting $u : \widetilde{E}(\mathbb{F}_p) \to E(\mathbb{Q}_p)$, let $\lambda_E(u)$ be a composition of the following maps

$$\lambda_E(u) : \widetilde{E}(\mathbb{F}_p) \stackrel{u}{\to} E(\mathbb{Q}_p) \stackrel{h}{\to} \mathbb{F}_p^+.$$

Satoh and Araki in [5, Theorem 3.2] showed that $\lambda_E(u)$ is a group homomorphism independent of the choice of u if $\widetilde{E}$ is anomalous (i.e. $N_p = p$). Then we can reduce the ECDLP over $\mathbb{F}_p$ to the DLP on $\mathbb{F}_p^+$ if $\widetilde{E}$ is anomalous. This is the idea of the anomalous attack.

3. The ECDLP over $\mathbb{Q}_p$

In the anomalous attack, the map h defined in §2 is a key tool. In this section, we generalize it with the filtration of the group $E_1(\mathbb{Q}_p)$ and give an algorithm for solving the ECDLP over $\mathbb{Q}_p$.

3.1. A Generalization of the Map h

Let p be a prime number and let E be an elliptic curve over $\mathbb{Q}_p$. Let $\widetilde{E}$ be the reduction curve of E over $\mathbb{F}_p$. For simplicity, we assume that $\widetilde{E}$ is an elliptic curve. For $n \geq 1$, we define a subgroup of $E(\mathbb{Q}_p)$ by

$$E_n(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) \mid v_p(x(P)) \leq -2n\} \cup \{O\},$$

where $x(P)$ is the x-coordinate of a point P. Note that $E_n(\mathbb{Q}_p)$ for $n = 1$ is the same as what we defined in §2. For $n \geq 1$, the subgroup $E_n(\mathbb{Q}_p)$ of $E_1(\mathbb{Q}_p)$ corresponds to the subgroup $\mathcal{E}(p^n\mathbb{Z}_p)$ of $\mathcal{E}(p\mathbb{Z}_p)$ under the isomorphism $E_1(\mathbb{Q}_p) \simeq \mathcal{E}(p\mathbb{Z}_p)$. Therefore we have the diagram

$$\begin{array}{ccc} E_1(\mathbb{Q}_p) & \simeq & \mathcal{E}(p\mathbb{Z}_p) \\ \cup & & \cup \\ E_2(\mathbb{Q}_p) & \simeq & \mathcal{E}(p^2\mathbb{Z}_p) \\ \cup & & \cup \\ E_3(\mathbb{Q}_p) & \simeq & \mathcal{E}(p^3\mathbb{Z}_p) \\ \cup & & \cup \\ \vdots & & \vdots \end{array}$$

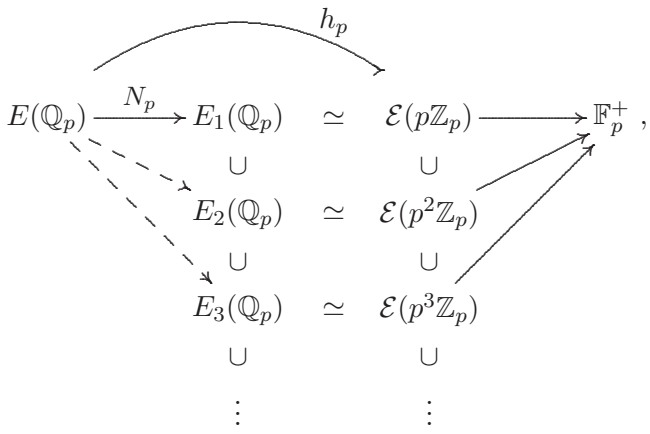
Moreover, we have that the map

$$\mathcal{E}(p^n\mathbb{Z}_p)/\mathcal{E}(p^{n+1}\mathbb{Z}_p) \xrightarrow{\mathrm{id}} p^n\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p \simeq \mathbb{F}_p^+ \tag{1}$$

is an isomorphism of groups for $n \geq 1$, where "id" denotes the identity map on sets (see [7, Proposition 3.2 of Chapter IV]). Therefore the group $E_1(\mathbb{Q}_p) \simeq \mathcal{E}(p\mathbb{Z}_p)$ has a filtration

$$\begin{array}{ccccccc} E_1(\mathbb{Q}_p) & \supset & E_2(\mathbb{Q}_p) & \supset & E_3(\mathbb{Q}_p) & \supset & \cdots \\ \| & & \| & & \| & & \\ \mathcal{E}(p\mathbb{Z}_p) & \supset & \mathcal{E}(p^2\mathbb{Z}_p) & \supset & \mathcal{E}(p^3\mathbb{Z}_p) & \supset & \cdots \\ & \mathbb{F}_p^+ & & \mathbb{F}_p^+ & & \mathbb{F}_p^+ & \end{array}$$

with isomorphisms (1). Then we can consider the following diagram:



where the maps on the right hand side are induced by isomorphisms (1). Since $\log_E(z) \equiv z \bmod z^2$ [7, §5 of Chapter IV], the first horizontal map is the same as the map h. Therefore we see that the above diagram is a generalization of the map h with the filtration of the group $E_1(\mathbb{Q}_p) \simeq \mathcal{E}(p\mathbb{Z}_p)$.

3.2. Our Algorithm

We here consider the ECDLP over $\mathbb{Q}_p$. Fix $S \in E(\mathbb{Q}_p)$ and $T \in \langle S \rangle$. If the order of S is finite, we have $\langle S \rangle \hookrightarrow \widetilde{E}(\mathbb{F}_p)$ in many cases and we can reduce the ECDLP over $\mathbb{Q}_p$ to the ECDLP over $\mathbb{F}_p$ (see [7, Example 6.11 of Chapter IV and Proposition 3.1 of Chapter VII]). Therefore we here assume that the order of S is infinite. Using the above diagram, we consider the method to solve the ECDLP over $\mathbb{Q}_p$ as follows:

1. We consider a composition of the following maps:

   $$h_p : E(\mathbb{Q}_p) \overset{N_p}{\to} E_1(\mathbb{Q}_p) \simeq \mathcal{E}(p\mathbb{Z}_p).$$

   Let h_1 be a composition of the following maps:

   $$h_1 : E(\mathbb{Q}_p) \overset{h_p}{\to} \mathcal{E}(p\mathbb{Z}_p) \to \mathbb{F}_p^+.$$

   We note that h_1 is equal to the map h defined in §2. Set $s_1 = h_1(S), t_1 = h_1(T) \in \mathbb{F}_p$. Compute $d_0 \in \mathbb{Z}$ with $0 \leq d_0 \leq p-1$ and $d_0 \equiv t_1 \cdot s_1^{-1} \bmod p$.

2. Set $S_1 = pS$ and $T_1 = T - d_0 S$. Then we have $h_p(S_1), h_p(T_1) \in \mathcal{E}(p^2\mathbb{Z}_p)$. We can transfer $h_p(S_1), h_p(T_1)$ to $s_2, t_2 \in \mathbb{F}_p$ like in Step 1. Compute $d_1 \in \mathbb{Z}$ with $0 \leq d_1 \leq p-1$ and $d_1 \equiv t_2 \cdot s_2^{-1} \bmod p$.

3. Set $S_2 = pS_1$ and $T_2 = T_1 - d_1 S_1$. Then we have $h_p(S_2), h_p(T_2) \in \mathcal{E}(p^3\mathbb{Z}_p)$. We compute $d_2 \in \mathbb{Z}$ like in Step 2.

4. We compute S_n, T_n and d_n until $T_n = 0$. Since

$$\begin{aligned} T_n &= T_{n-1} - d_{n-1}S_{n-1} \\ &= (T_{n-2} - d_{n-2}S_{n-2}) - d_{n-1}pS_{n-2} \\ &= T_{n-2} - (d_{n-2} + d_{n-1}p)S_{n-2} \\ &\cdots \\ &= T - \sum_{i=0}^{n-1} d_i p^i S, \end{aligned}$$

we have $T = dS$ with $d = \sum_{i=0}^{n-1} d_i p^i$.

For any point $Q \in E(\mathbb{Q}_p)$, we have

$$h_p(Q) = -\frac{x}{y} \in \mathcal{E}(\mathbb{Q}_p)$$

with $N_p Q = (x, y)$ (see [7, §2 of Chapter VII]). Therefore we can give an algorithm for solving the ECDLP over $\mathbb{Q}_p$ in Algorithm 1. Note that we mainly need the following operations to compute Algorithm 1:

- counting the order of the reduced elliptic curve $\widetilde{E}$ over $\mathbb{F}_p$ (Step 1).
- group operations on E over $\mathbb{Q}_p$ (Step 5 and Step 8).

Remark. In Algorithm 1, we assume that $h_p(S) \notin E_2(\mathbb{Q}_p)$ for simplicity. In the case $h_p(S) \in E_2(\mathbb{Q}_p)$, we have $h_p(S) \notin E_k(\mathbb{Q}_p)$ for some k since the order of S is infinite. Therefore we can easily reconstruct Algorithm 1 in this case.

In Algorithm 1, the integer sequence $\{d_i\}_{0 \le i \le n-1}$ satisfies $d = \sum_{i=0}^{n-1} d_k p^k$ with $0 \le d_i \le p-1$. Therefore the expected number of iterations in Step 4 is estimated at $\log_p d$. Hence it takes approximately

$$(\text{counting } \widetilde{E}(\mathbb{F}_p)) + 2\log_p d \cdot \log p \cdot A$$

to compute Algorithm 1, where A denote a group operation on E over $\mathbb{Q}_p$. Moreover, if we assume that $d < M$ for some M, it takes approximately

$$(\text{counting } \widetilde{E}(\mathbb{F}_p)) + 2\log_p M \cdot \log p \cdot A$$

Algorithm 1 Solving the ECDLP over $\mathbb{Q}_p$

Require: (E, S, T), where E is an elliptic curve defined over $\mathbb{Q}_p$ with good reduction, $S \in E(\mathbb{Q}_p)$ of infinite order and $T \in \langle S \rangle$. For simplicity, we assume that $h_p(S) \notin E_2(\mathbb{Q}_p)$.

Ensure: The integer d with $T = dS$.

1: $N_p \leftarrow \sharp\widetilde{E}(\mathbb{F}_p)$, where $\widetilde{E}$ is the reduced elliptic curve of E.
2: Compute $N_pS = (x, y)$ and set $a = -\frac{x}{py} \bmod p$. By the assumption $h_p(S) \notin E_2(\mathbb{Q}_p)$, we have $a \not\equiv 0 \bmod p$.
3: Set $n = 0, \ell = 1, S' = S, T' = T$.
4: **while** $T' \neq 0$ **do**
5: Compute $N_pT' = (x, y)$ and set $w = -\frac{x}{y}$.
6: Set $b = \frac{w}{p^\ell}$.
7: Compute $d_n = b \cdot a^{-1} \bmod p$ and let d_n with $0 \leq d_n \leq p-1$ and $d_n \equiv \bar{d_n} \bmod p$.
8: $T' \leftarrow T' - d_nS', S' \leftarrow pS'$.
9: $n \leftarrow n + 1, \ell \leftarrow \ell + 1$.
10: **end while**
11: Compute $d = \sum_{i=0}^{n-1} d_i p^i$.
12: Return d.

to compute Algorithm 1.

In general, it takes very long time to compute a group operation on E over $\mathbb{Q}_p$. However, in the following example, we can compute the integer d with $T = dS$ using group operations on $E \bmod p^5$.

Example. Suppose $p = 547,\ E : y^2 = x^3 + 3x$ and $S = (x_1, y_1)$ with

$$\begin{cases} x_1 = 137 + 410p + 136p^2 + 410p^3 + 136p^4 + O(p^5), \\ y_1 = 341 + 478p + 341p^2 + 478p^3 + 341p^4 + O(p^5). \end{cases}$$

For a randomly chosen d, let $T = dS = (x_2, y_2)$ be a point of $\langle S \rangle$ defined by

$$\begin{cases} x_2 = 97 + 358p + 346p^2 + 320p^3 + 323p^4 + O(p^5), \\ y_2 = 47 + 512p + 514p^2 + 409p^3 + 431p^4 + O(p^5). \end{cases}$$

In the notation of Algorithm 1, we have $d_0 = 508,\ d_1 = 46,\ d_2 = 1$. Therefore we obtain $d = d_0 + d_1p + d_2p^2 = 324879$ with $T = dS$.

Remark. Let E be an elliptic curve defined over $\mathbb{Q}$. Fix a prime p at which E has good reduction. Considering $E(\mathbb{Q}) \hookrightarrow E(\mathbb{Q}_p)$, we can solve the

ECDLP over $\mathbb{Q}$ by applying Algorithm 1 as follows: Let E be an elliptic curve $\mathbb{Q}$ given by the Weierstrass equation

$$E : y^2 + y = x^3 - x.$$

The Mordell-Weil group $E(\mathbb{Q})$ has rank 1 and a point $S = (0, 0)$ is a generator for $E(\mathbb{Q})$. Moreover, the elliptic curve E has good reduction outside 37. For randomly chosen d, let $T = dS = (x_T, y_T)$ be a point of $E(\mathbb{Q})$ defined by

$$\begin{aligned} x_T &= -\frac{3148929681285740316}{2846153597907293521}, \\ y_T &= -\frac{2181616293371330311419201915}{480161683557909927586282743 1}. \end{aligned}$$

Then we have the followings:

- In the case $p = 3$, Algorithm 1 gives $d_0 = 2, d_1 = 0, d_2 = 0, d_3 = 1$ and $d = 2 + 0 \cdot p + 0 \cdot p^2 + 1 \cdot p^3 = 29$.
- In the case $p = 5$, Algorithm 1 gives $d_0 = 4, d_1 = 0, d_2 = 1$ and $d = 4 + 0 \cdot p + 1 \cdot p^2 = 29$.

In each cases, we have $d = 29$ with $T = dS$.

4. Conclusion

Let E be an elliptic curve over $\mathbb{Q}_p$. The map $h : E(\mathbb{Q}_p) \to \mathbb{F}_p^+$ defined in §2 is a key tool in the anomalous attack (see [5] for details). Considering the filtration of the group $E_1(\mathbb{Q}_p) \simeq \mathcal{E}(p\mathbb{Z}_p)$, we generalized the map h and gave Algorithm 1 for solving the ECDLP over $\mathbb{Q}_p$.

5. Remarks

The preliminary version of this paper was included in the proceedings of ISPEC 2010 [9].

References

[1] I.F. Blake, G. Seroussi, N.P. Smart, *Elliptic Curves in Cryptography*, Cambridge University Press (1999).

[2] D. Hankerson, A. Menezes, S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer-Verlag, New York (2004).

[3] N. Koblitz, Elliptic curve cryptosystems, *Mathematics of Computation*, **48** (1987), 203-209.

[4] V.S. Miller, Use of elliptic curves in cryptography, *Advances in Cryptology CRYPTO '85, LNCS 218*, Springer-Verlag (1986), 417-426.

[5] T. Satoh, K. Araki, Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves, *Commentarii Mathematici Universitatis Sancti Pauli*, **47** (1998), 81-92.

[6] I. Semaev, Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p, *Mathematics of Computation*, **67** (1998), 353-356.

[7] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math., Springer-Verlag, Berlin-Heidelberg-New York (1986).

[8] N.P. Smart, The discrete logarithm problem on elliptic curves of trace one, *Journal of Cryptology*, **12** (1999), 110-125.

[9] M. Yasuda, The elliptic curve discrete logarithm problems over the p-adic fields and formal groups, *ISPEC 2010, LNCS 6047* (2010), 110-122.